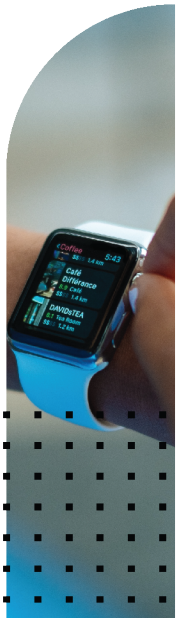
Release Notes

FortiManager 7.0.2



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

October 22, 2021
FortiManager 7.0.2 Release Notes
02-702-752007-20211022

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-10-20	Initial release.
2021-10-22	Updated Appendix B - Default and maximum number of ADOMs supported on page 47.

FortiManager 7.0.2 Release

This document provides information about FortiManager version 7.0.2 build 0180.

The recommended minimum screen resolution for the FortiManager GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

This section includes the following topics:

Supported models

FortiManager version 7.0.2 supports the following models:

FortiManager	FMG-200F, FMG-200G, FMG-300F, FMG-400E, FMG-1000F, FMG-2000E FMG-3000F, FMG-3000G, FMG-3700F, and FMG-3900E.
FortiManager VM	FMG_DOCKER, FMG-VM64, FMG-VM64-AWS, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-HV (including Hyper-V 2016, 2019), FMG-VM64-KVM, FMG-VM64-OPC, FMG-VM64-XEN (for both Citrix and Open Source Xen).

FortiManager VM subscription license

The FortiManager VM subscription license supports FortiManager version 6.4.1 and later. For information about supported firmware, see FortiManager VM firmware on page 13.

See also Appendix B - Default and maximum number of ADOMs supported on page 47.

You can use the FortiManager VM subscription license with new FMG-VM installations.

For existing FMG-VM installations, you cannot upgrade to a FortiManager VM subscription license. Instead, you must migrate data from the existing FMG-VM to a new FMG-VM with subscription license.

Management extension applications

The following section describes supported models and minimum system requirements for management extension applications (MEA) in FortiManager7.0.2.

FortiManager uses port TCP/443 or TCP/4443 to connect to the Fortinet registry and download MEAs. Ensure that the port is also open on any upstream FortiGates. For more information about incoming and outgoing ports, see the FortiManager 7.0 Ports Guide.

Supported models for MEA

You can use any of the following FortiManager models as a host for management extension applications:

FortiManager	FMG-3000F, FMG-3000G, FMG-3700F, and FMG-3900E.
FortiManager VM	FMG_DOCKER, FMG-VM64, FMG-VM64-AWS, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-HV (including Hyper-V 2016, 2019), FMG-VM64-KVM, FMG-VM64-OPC, FMG-VM64-XEN (for both Citrix and Open Source Xen).

Minimum system requirements

By default FortiManager VMs use the following system resource settings:

- 4 vCPU
- 8 GB RAM
- 500 GB disk space

Starting with FortiManager 7.0.0, RAM and CPU is capped at 50% for MEAs. (Use the `config system docker` command to view the setting.) If FortiManager has 8 CPUs and 16 GB RAM, then only 4 CPUs and 8 GB RAM are available to MEAs by default, and the 4 CPUs and 8 GB RAM are used for all enabled MEAs.

Some management extension applications have minimum system requirements that require you to increase system resources. The following table identifies the minimum requirements for each MEA as well as the recommended system resources to function well in a production environment.

MEA minimum system requirements apply only to the individual MEA and do not take into consideration any system requirements for resource-sensitive FortiManager features or multiple, enabled MEAs. If you are using multiple MEAs, you must increase the system resources to meet the cumulative need of each MEA.

Management Extension Application	Minimum system requirements	Recommended system resources for production*
FortiAIOps	• 8 vCPU • 32 GB RAM • 500 GB disk storage	No change
FortiAuthenticator	• 4 vCPU	No change

Management Extension Application	Minimum system requirements	Recommended system resources for production*
	• 8 GB RAM	
FortiPortal	• 4 vCPU • 8 GB RAM	No change
FortiSigConverter	• 4 vCPU • 8 GB RAM	No change
FortiSOAR	• 4 vCPU • 8 GB RAM • 500 GB disk storage	• 16 vCPU • 64 GB RAM • No change for disk storage
Policy Analyzer	• 4 vCPU • 8 GB RAM	No change
SD-WAN Orchestrator	• 4 vCPU • 8 GB RAM	• 4 vCPU • 12 GB RAM
Universal Connector	• 1 GHZ vCPU • 2 GB RAM • 1 GB disk storage	No change
Wireless Manager (FortiWLM)	• 4 vCPU • 8 GB RAM	No change

*The numbers in the *Recommended system resources for production* column are a combination of the default system resource settings for FortiManager plus the minimum system requirements for the MEA.

Special Notices

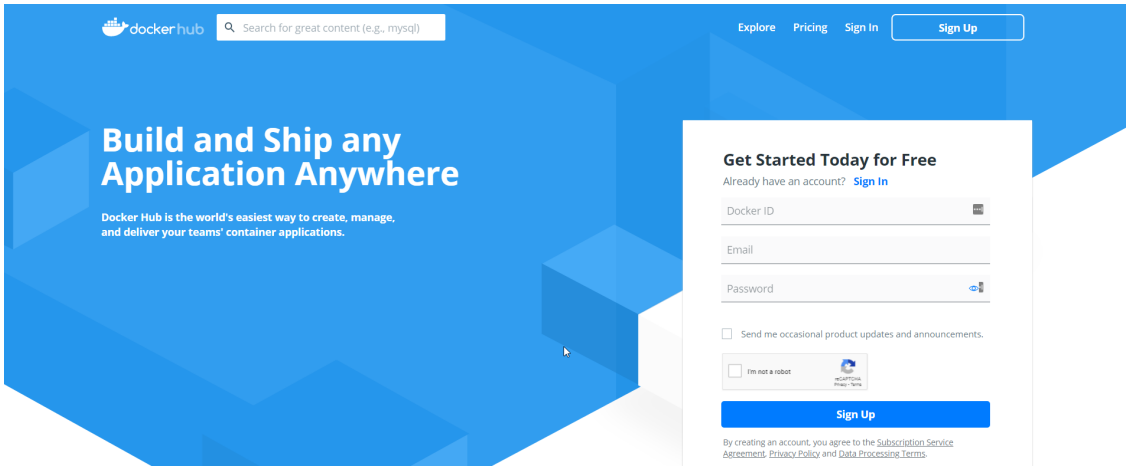
This section highlights some of the operational changes that administrators should be aware of in 7.0.2.

Fortinet verified publisher docker image

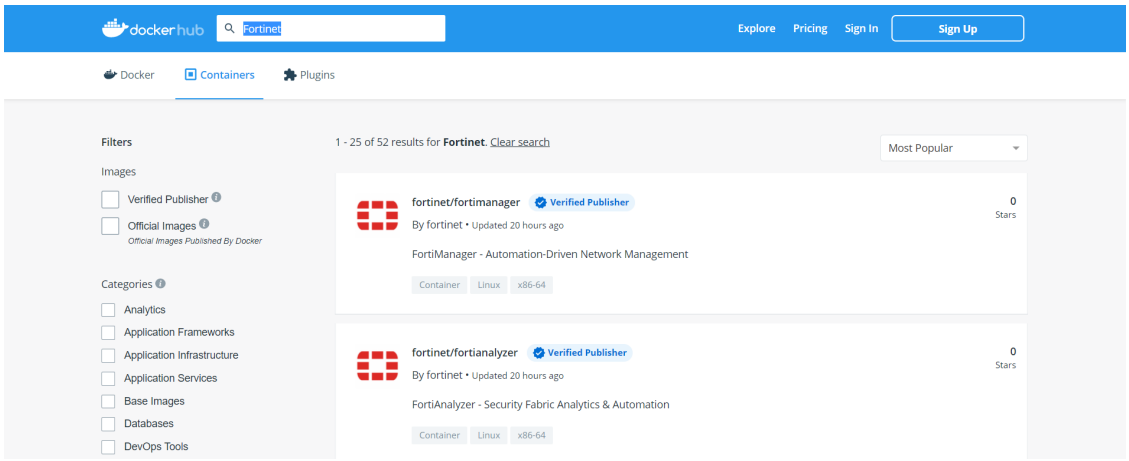
FortiManager 7.0.1 docker image is available for download from Fortinet's Verified Publisher public repository on dockerhub.

To download the FortiManager image from dockerhub:

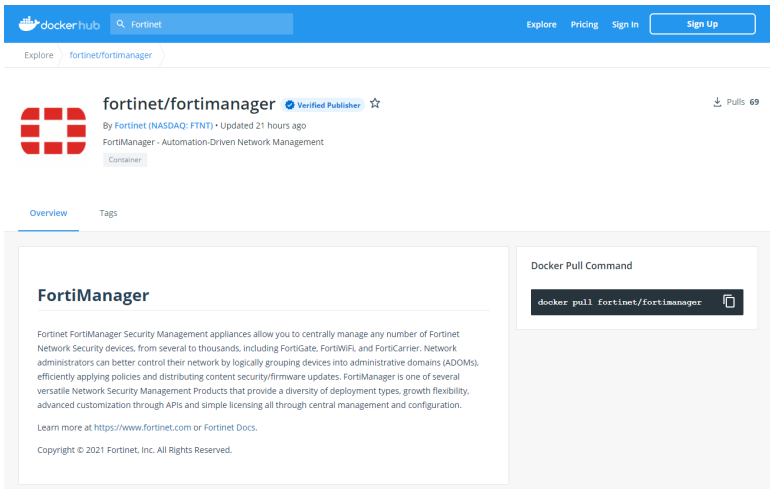
1. Go to dockerhub at https://hub.docker.com/.
   The dockerhub home page is displayed.



2. In the banner, click *Explore*.
3. In the search box, type *Fortinet*, and press *Enter*.
   The *fortinet/fortimanager* and *fortinet/fortianalyzer* options are displayed.



4. Click *fortinet/fortimanager*.
   The *fortinet/fortimanager* page is displayed, and two tabs are available: *Overview* and *Tags*. The *Overview* tab is selected by default.



5. On the *Overview* tab, copy the docker pull command, and use it to download the image.
   The CLI command from the *Overview* tab points to the latest available image. Use the *Tags* tab to access different versions when available.

Scheduling firmware upgrades for managed devices

Starting in FortiManager 7.0.0, firmware templates should be used to schedule firmware upgrades on managed FortiGates. Attempting firmware upgrade from the FortiManager GUI by using legacy methods may ignore the *schedule upgrade* option and result in FortiGates being upgraded immediately.

Modifying the interface status with the CLI

Starting in verion 7.0.1, the CLI to modify the interface status has been changed from `up`/`down` to `enable`/`disable`.

For example:

```
config system interface
   edit port2
      set status <enable/disable>
   next
end
```

SD-WAN with upgrade to 7.0

Due to design change with SD-WAN Template, upgrading to FortiManager 7.0 may be unable to maintain dynamic mappings for all SD-WAN interface members. Please reconfigure all the missing interface mappings after upgrade.

Citrix XenServer default limits and upgrade

Citrix XenServer limits ramdisk to 128M by default. However the FMG-VM64-XEN image is larger than 128M. Before updating to FortiManager 6.4, increase the size of the ramdisk setting on Citrix XenServer.

To increase the size of the ramdisk setting:

1. On Citrix XenServer, run the following command:
   ```
   xenstore-write /mh/limits/pv-ramdisk-max-size 536,870,912
   ```
2. Confirm the setting is in effect by running `xenstore-ls`.
   ```
   ----------------------
   limits = ""
   pv-kernel-max-size = "33554432"
   pv-ramdisk-max-size = "536,870,912"
   boot-time = ""
   ---------------------------
   ```
3. Remove the pending files left in `/run/xen/pygrub`.

The ramdisk setting returns to the default value after rebooting.

Multi-step firmware upgrades

Prior to using the FortiManager to push a multi-step firmware upgrade, confirm the upgrade path matches the path outlined on our support site. To confirm the path, please run:

```
dia fwmanager show-dev-upgrade-path <device name> <target firmware>
```

Alternatively, you can push one firmware step at a time.

Hyper-V FortiManager-VM running on an AMD CPU

A Hyper-V FMG-VM running on a PC with an AMD CPU may experience a kernel panic. Fortinet recommends running VMs on an Intel-based PC.

SSLv3 on FortiManager-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiManager-VM64-AWS only enables TLSv1 by default. All other models enable both TLSv1 and SSLv3. If you wish to disable SSLv3 support, please run:

```
config system global
set ssl-protocol t1sv1
```

```
    end
```

Upgrade Information

You can upgrade FortiManager 6.4.0 or later directly to 7.0.2.

For other upgrade paths and details about upgrading your FortiManager device, see the *FortiManager Upgrade Guide*.

This section contains the following topics:

Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous firmware release via the GUI or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset {all-settings | all-except-ip}
execute format {disk | disk-ext4 | disk-ext3}
```

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

FortiManager VM firmware

Fortinet provides FortiManager VM firmware images for Amazon AWS, Citrix and Open Source XenServer, Linux KVM, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

Amazon Web Services

- The 64-bit Amazon Machine Image (AMI) is available on the AWS marketplace.

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the QCOW2 file for the Open Source Xen Server.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Google Cloud Platform

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.gcp.zip`: Download the 64-bit package for a new FortiManager VM installation.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains QCOW2 that can be used by qemu.

Microsoft Azure

The files for Microsoft Azure have AZURE in the filenames, for example `FMG_VM64_AZURE-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.

Microsoft Hyper-V Server

The files for Microsoft Hyper-V Server have HV in the filenames, for example, `FMG_VM64_HV-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.

Microsoft Hyper-V 2016 is supported.

Oracle Private Cloud

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.opc.zip`: Download the 64-bit package for a new FortiManager VM installation.

VMware ESX/ESXi

- `.out`: Download the 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

For more information see the FortiManager Data Sheet available on the Fortinet web site. VM installation guides are available in the Fortinet Document Library.

SNMP MIB files

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiManager version 5.00 file folder.

Product Integration and Support

This section lists FortiManager 7.0.2 support of other Fortinet products. It also identifies what FortiManager features are supported for managed platforms and what languages FortiManager supports. It also lists which Fortinet models can be managed by FortiManager.

The section contains the following topics:

FortiManager 7.0.2 support

This section identifies FortiManager 7.0.2 product integration and support information:

To confirm that a device model or firmware version is supported by the current firmware version running on FortiManager, run the following CLI command:

```
diagnose dvm supported-platforms list
```

Always review the Release Notes of the supported platform firmware version before upgrading your device.

Web browsers

This section lists FortiManager 7.0.2 product integration and support for web browsers:

- Microsoft Edge 80 (80.0.361 or later)
- Mozilla Firefox version 93
- Google Chrome version 94

Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS/FortiOS Carrier

This section lists FortiManager 7.0.2 product integration and support for FortiOS/FortiOS Carrier:

- 7.0.0 to 7.0.2
- 6.4.0 to 6.4.7
- 6.2.0 to 6.2.9

FortiADC

This section lists FortiManager 7.0.2 product integration and support for FortiADC:

- 6.0.1
- 5.4.5

FortiAnalyzer

This section lists FortiManager 7.0.2 product integration and support for FortiAnalyzer:

- 7.0.0 and later
- 6.4.0 and later
- 6.2.0 and later
- 6.0.0 and later
- 5.6.0 and later
- 5.4.0 and later

FortiAuthenticator

This section lists FortiManager 7.0.2 product integration and support for FortiAuthenticator:

- 6.0 to 6.2
- 5.0 to 5.5
- 4.3.0 and later

FortiCache

This section lists FortiManager 7.0.2 product integration and support for FortiCache:

- 4.2.9
- 4.1.6
- 4.0.4

FortiClient

This section lists FortiManager 7.0.2 product integration and support for FortiClient:

- 6.4.0 and later
- 6.2.1 and later
- 6.0.0 and later

FortiDDoS

This section lists FortiManager 7.0.2 product integration and support for FortiDDoS:

- 5.5.0
- 5.4.2
- 5.3.1
- 5.2.0
- 5.1.0
- 5.0.0
- 4.7.0
- 4.6.0
- 4.5.0
- 4.4.2
- 4.3.2
- 4.2.3

Limited support. For more information, see Feature support on page 20.

FortiMail

This section lists FortiManager 7.0.2 product integration and support for FortiMail:

- 6.4.0 and later
- 6.2.0 and later
- 6.0.10 and later
- 5.4.12
- 5.3.13

FortiSandbox

This section lists FortiManager 7.0.2 product integration and support for FortiSandbox:

- 4.0.1
- 3.2.3

- 3.1.4
- 3.0.6
- 2.5.2
- 2.4.1
- 2.3.3
- 2.2.2

FortiSOAR

This section lists FortiManager 7.0.2 product integration and support for FortiSOAR:

- 6.4.0 and later
- 6.0.0 and later

FortiSwitch ATCA

This section lists FortiManager 7.0.2 product integration and support for FortiSwitch ATCA:

- 5.2.3
- 5.0.0 and later

FortiTester

This section lists FortiManager 7.0.2 product integration and support for FortiTester:

- 7.0
- 4.2
- 4.1
- 4.0
- 3.9
- 3.8
- 3.7

FortiWeb

This section lists FortiManager 7.0.2 product integration and support for FortiWeb:

- 6.3.13
- 6.2.4
- 6.1.2
- 6.0.7
- 5.9.1
- 5.8.6
- 5.7.3
- 5.6.2

- 5.5.7
- 5.4.1

Virtualization

This section lists FortiManager 7.0.2 product integration and support for virtualization:

- Amazon Web Service AMI, Amazon EC2, Amazon EBS
- Citrix XenServer 7.2
- Google Cloud Platform
- Linux KVM Redhat 7.1
- Microsoft Azure
- Microsoft Hyper-V Server 2012 and 2016
- Nutanix AHV (AOS 5.10.5)
- OpenSource XenServer 4.2.5
- Oracle Private Cloud
- VMware ESXi versions 5.0, 5.5, 6.0, 6.5 , 6.7, and 7.0

Feature support

The following table lists FortiManager feature support for managed platforms.

Platform	Management Features	FortiGuard Update Services	Reports	Logging
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓
FortiADC		✓		
FortiAnalyzer			✓	✓
FortiAuthenticator				✓
FortiCache			✓	✓
FortiClient		✓	✓	✓
FortiDDoS			✓	✓
FortiMail		✓	✓	✓
FortiSandbox		✓	✓	✓
FortiSOAR		✓		
FortiSwitch ATCA	✓			
FortiWeb		✓	✓	✓
Syslog				✓

Language support

The following table lists FortiManager language support information.

Language	GUI	Reports
English	✓	✓
Chinese (Simplified)	✓	✓
Chinese (Traditional)	✓	✓
French		✓
Japanese	✓	✓
Korean	✓	✓
Portuguese		✓
Spanish		✓

To change the FortiManager language setting, go to *System Settings* > *Admin* > *Admin Settings*, in *Administrative Settings* > *Language* select the desired language on the drop-down menu. The default value is *Auto Detect*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can create your own language translation files for these languages by exporting a predefined language from FortiManager, modifying the text to a different language, saving the file as a different language name, and then importing the file into FortiManager. For more information, see the *FortiAnalyzer Administration Guide*.

Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, FortiCache, FortiProxy, and FortiAuthenticator models and firmware versions that can be managed by a FortiManager or send logs to a FortiManager running version 7.0.2.

Software license activated LENC devices are supported, if their platforms are in the supported models list. For example, support of FG-3200D indicates support of FG-3200D-LENC.

This section contains the following topics:

FortiGate models

Model	Firmware Version
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60EDSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate80E-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate301E, FortiGate-400D, FortiGate-400E, FortiGate-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2200E, FortiGate2201E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate3960E, FortiGate-3980E **FortiGate 5000 Series**: FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 **FortiGate DC**: FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC **FortiWiFi**: FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F **FortiGate VM**: FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-AZURE, FortiGate-VM64-GCP, FortiGate-VM64-HV,FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGateVM64-Xen, FortiGate-VMX-Service-Manager, FortiGate-VM64-IBM **FortiOS**: FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen **FortiGateRugged**: FortiGateRugged-60F, FortiGateRugged-60F-3G4G	7.0

Model	Firmware Version
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate-80E-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-2200E, FortiGate-2201E, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E **FortiGate 5000 Series:** FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 **FortiGate DC:**FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC **FortiGate Hardware Low Encryption:** FortiGate-100D-LENC **FortiWiFi:** FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-61E, FortiWiFi-60F, FortiWiFi-61F, **FortiGate VM:** FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-AZURE, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV,FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager, FortiGate-VM64-IBM **FortiOS:** FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen **FortiGateRugged:** FortiGateRugged-60F, FortiGateRugged-60F-3G4G	6.4
FortiGate: FortiGate-30E, FortiGate-30E-3G4G-INTL, FortiGate-30E-3G4G-NAM, FortiGate-40F, FortiGate-40F-3G4G, FortiGate-50E, FortiGate-51E, FortiGate-52E, FortiGate-60E, FG-60E-DSL, FortiGate-60E-POE, FortiGate-61E, FortiGate-60F, FortiGate-61F, FortiGate-80D, FortiGate-80E, FortiGate-80E-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-92D, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-101E, FortiGate-100F, FortiGate-101F, FortiGate-140D, FortiGate-140D-POE, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FG-400E, FG-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-1100E, FortiGate-1101E, FortiGate-2000E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3700D, FortiGate-3800D,FortiGate-2200E, FortiGate-2201E, FortiGate-2200E, FortiGate-2201E, FortiGate-3300E, FortiGate-3301E, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E **FortiGate 5000 Series:** FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 **FortiGate 7000 Series:** FortiGate-7000F	6.2

Model	Firmware Version
FortiGate DC: FortiGate-80C-DC, FortiGate-401E-DC, FortiGate-600C-DC, RortiGate-800C-DC, FortiGate-800D-DC, FortiGate-1000C-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3240C-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600C-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC **FortiGate Hardware Low Encryption:** FortiGate-80C-LENC, FortiGate-600C-LENC, FortiGate-1000C-LENC **FortiWiFi:** FortiWiFi-30D, FortiWiFi-30D-POE, FortiWiFi-30E, FortiWiFi-30E-3G4G-INTL, FortiWiFi-30E-3G4G-NAM, FortiWiFi-50E, FortiWiFi-50E-2R, FortiWiFi-51E, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-61E, FortiWiFi-80CM, FortiWiFi-81CM, FortiWiFi-60F, FortiWiFi-61F **FortiGate-VM:** FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-ALIONDEMAND, FortiGate-VM64-AWS, FortiGate-VM64-AWSONDEMAND, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager **FortiGate Rugged:** FortiGateRugged-30D, FortiGateRugged-30D-ADSL-A, FortiGateRugged-35D, FortiGateRugged-60F, FortiGateRugged-60F-3G4G **FortiOS:** FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen	

FortiGate special branch models

The following FortiGate models are released on special branches of FortiOS. FortiManager version 7.0.2 supports these models on the identified FortiOS version and build number.

FortiOS 6.4

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-80F-POE, FortiGate-81F-POE	6.4.7	5944
FortiGate-200F	6.4.6	5785
FortiGate-1800F, FortiGate-1800F-DC	6.4.6	5866
FortiGate-1801F, FortiGate-1801F-DC	6.4.6	5868
FortiGate-2600F, FortiGate-2600F-DC	6.4.6	5866
FortiGate-2601F, FortiGate-2601F-DC	6.4.6	5868
FortiGate-3500F	6.4.6	5886
FortiGate-3501F	6.4.6	5876
FortiGate-4200F, FortiGate-4200F-DC FortiGate-4201F, FortiGate-4201F-DC	6.4.6	5868

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-4400F, FortiGate-4400F-DC FortiGate-4401F, FortiGate-4401F-DC		
FortiWiFi-80F-2R FortiWiFi-81F-2R FortiWiFi-81F-2R-3G4G-POE FortiWiFi-81F-2R-POE	1911	5944
FortiGate-6000F	6.4.6	1766
FortiGate-7000E, FortiGate-7000F	6.4.6	1766

FortiOS 6.2

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-80F-POE, FortiGate-81F-POE	6.2.6	7097
FortiGate-200F, FortiGate-201F	6.2.8	7088
FortiGate-1800F, FortiGate-1800F-DC FortiGate-1801F, FortiGate-1801F-DC	6.2.7	7104
FortiGate-2600F, FortiGate-2600F-DC FortiGate-2601F, FortiGate-2601F-DC	6.2.7	7104
FortiGate-4200F, FortiGate-4200F-DC FortiGate-4201F, FortiGate-4201F-DC	6.2.7	7104
FortiGate-4400F, FortiGate-4400F-DC	6.2.7	7105
FortiGate-4401F, FortiGate-4401F-DC	6.2.7	7104
FortiWiFi-80F-2R FortiWiFi-81F-2R	6.2.6	6997
FortiWiFi-81F-2R-3G4G-POE	6.2.6	7099
FortiWiFi-81F-2R-POE	6.2.6	7032
FortiGate-6000F	6.2.6	1158
FortiGate-7000E	6.2.6	1158

FortiCarrier models

Model	Firmware Version
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FotiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 **FortiCarrier-DC**: FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC **FortiCarrier-VM**: FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	7.0
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3400E, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 **FortiCarrier-DC:** FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC **FortiCarrier-VM:** FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	6.4
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 **FortiCarrier-DC:** FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC **FortiCarrier-VM:** FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	6.2

FortiADC models

Model	Firmware Version
FortiADC-100F, FortiADC-200D, FortiADC-200F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-4000D, FortiADC-4000F, FortiADC-5000F, FortiADC-VM	6.0

Model	Firmware Version
FortiADC-100F, FortiADC-200D, FortiADC-200F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-4000D, FortiADC-4000F, FortiADC-5000F, FortiADC-VM	5.4

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FortiAnalyzer-150G, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3900E **FortiAnalyzerVM**: FortiAnalyzer-VM64, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	7.0
FortiAnalyzer: FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-1000E, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3900E **FortiAnalyzer VM:** FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-ALI-OnDemand, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWSOnDemand, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-GCP-OnDemand,FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-KVM-CLOUD, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	6.4
FortiAnalyzer: FAZ-200F, FAZ-300F, FAZ-400E, FAZ-800F, FAZ-1000E, FAZ-2000E, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3700F and FAZ-3900E. **FortiAnalyzer VM:** FAZ-VM64, FAZ-VM64-Ali, FAZ-VM64-AWS, FAZ-VM64-AWS-OnDemand, FAZ-VM64-Azure, FAZ-VM64-GCP, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-OPC, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	6.2
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E. **FortiAnalyzer VM:** FAZ-VM64, FAZ-VM64-AWS, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	6.0
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E. **FortiAnalyzer VM:** FAZ-VM64, FAZ-VM64-AWS, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	5.6

Model	Firmware Version
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, and FAZ-4000B. **FortiAnalyzer VM:** FAZ-VM64, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-XEN (Citrix XenServer and Open Source Xen), FAZ-VM64-KVM, and FAZ-VM64-AWS.	5.4

FortiAuthenticator models

Model	Firmware Version
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000D, FAC-3000E **FortiAuthenticator VM:** FAC-VM	6.0 to 6.2
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000B, FAC-3000D, FAC-3000E **FortiAuthenticator VM:** FAC-VM	5.0 to 5.5
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-3000B, FAC-3000D, FAC-3000E **FortiAuthenticator VM:** FAC-VM	4.3

FortiCache models

Model	Firmware Version
FortiCache: FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3000E, FCH-3900E **FortiCache VM:** FCH-VM64, FCH-KVM	4.0, 4.1, 4.2

FortiDDoS models

Model	Firmware Version
FortiDDoS: FortiDDoS-200B, FortiDDoS-400B, FortiDDoS-600B, FortiDDoS-800B, FortiDDoS-900B, FortiDDoS-1000B, FortiDDoS-1200B, FortiDDoS-1500E, FortiDDoS-2000B, FortiDDoS-2000E	5.2, 5.3
FortiDDoS: FI-200B, FI-400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-1500B, FI-2000B, FI-2000E	5.1
FortiDDoS: FI-1500E, FI-2000E	5.0
FortiDDoS: FI-200B, FI400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-2000B, FI-3000B	4.2, 4.3, 4.4, 4.5, 4.7

FortiMail models

Model	Firmware Version
FortiMail: FE-60D, FE-200D, FE-200E, FE-400E, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM, FML-200F, FML-400F, FML-900F	6.0
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000E, FE-3200E **FortiMail Low Encryption:** FE-3000C-LENC	5.4
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000D, FE-3000E, FE-3200E, FE-5002B **FortiMail Low Encryption:** FE-3000C-LENC **FortiMail VM:** FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.3

FortiProxy models

Model	Firmware Version
FortiProxy: FPX-400E, FPX-2000E, FPX-4000E **FortiProxy VM:** FPX-KVM, FPX-VM64	1.0, 1.1, 1.2

FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-500F, FSA-1000F, FSA-2000E, FSA-3000E **FortiSandbox-VM:** FSA-AWS, FSA-VM	4.0
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox-VM:** FSA-AWS, FSA-VM	3.2
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox-VM:** FSA-AWS, FSA-VM	3.1
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox VM:** FSA-AWS, FSA-VM	3.0
FortiSandbox: FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox VM:** FSA-KVM, FSA-VM	2.5.2

Model	Firmware Version
FortiSandbox: FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox VM:** FSA-VM	2.4.1 2.3.3
FortiSandbox: FSA-1000D, FSA-3000D, FSA-3500D **FortiSandbox VM:** FSA-VM	2.2.0

FortiSOAR models

Model	Firmware Version
FortiSOAR VM: FSR-VM	6.4
FortiSOAR VM: FSR-VM	6.0

FortiSwitch ATCA models

Model	Firmware Version
FortiController: FTCL-5103B, FTCL-5902D, FTCL-5903C, FTCL-5913C	5.2.0
FortiSwitch-ATCA: FS-5003A, FS-5003B **FortiController:** FTCL-5103B, FTCL-5903C, FTCL-5913C	5.0.0

FortiTester models

Model	Firmware Version
FortiTester: FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2500E, FortiTester-3000E, FortiTester-4000E **FortiTester VM:** FortiTester-VM, FortiTester-VM-ALI-BYOL	3.9
FortiTester: FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2500E, FortiTester-3000E, FortiTester-4000E **FortiTester VM:** FortiTester-VM, FortiTester-VM-ALI-BYOL	3.8
FortiTester: FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2500E, FortiTester-3000E, FortiTester-4000E **FortiTester VM:** FortiTester-VM, FortiTester-VM-ALI-BYOL	3.7

FortiWeb models

Model	Firmware Version
FortiWeb: FortiWeb-100D, FortiWeb-400C, FortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E **FortiWeb VM:** FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	6.2, 6.3
FortiWeb: FortiWeb-100D, FortiWeb-400C, FortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E **FortiWeb VM:** FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-Docker, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XenServer	6.1
FortiWeb: FWB-100D, FWB-400C, FWB-400D, FWB-600D, FWB-1000D, FWB-1000E, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM, FWB-HYPERV, FWB-XENOPEN, FWB-XENSERVER	6.0.1
FortiWeb: FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.9.1
FortiWeb: FWB-1000C, FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-Azure-Ondemand, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.8.6
FortiWeb: FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-OS1, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.7.2
FortiWeb: FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.6.1

Model	Firmware Version
FortiWeb: FWB-100D, FWB-400C, FWB-400D, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM-64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, FWB-HYPERV, FWB-KVM, FWB-AZURE	5.5.6
FortiWeb: FWB-100D, FWB-400C, FWB-1000C, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, FWB-HYPERV	5.4.1

Resolved Issues

The following issues have been fixed in 7.0.2. For inquires about a particular bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
673020	Creating SSID interface with central AP Manager automatically generates normalized interface name that has no default mapping configuration.
702114	FortiManager is unable to see 5Ghz Clients in *Health Monitor*.

Device Manager

Bug ID	Description
563690	Device Manager fails to add FortiAnalyzer that contains a FortiGate HA device with error: *serial number does not match database*.
609859	When installing device settings, the default name for downloaded preview file should be more identifiable for a device.
637388	System Dashboard's time zones are not sorted within the dropdown list.
638750	*Where Used* may not work for IPsec Phase 2 allowing users to delete used objects.
662095	FortiManager may take too much time to send SLA updates to over thousands of FortiGate devices.
665207	FortiManager needs IPv6 support on Syslog server setting.
691611	FortiManager does `auto-retrieve` and causes all policy package statuses to become *unknown* after a new VDOM is created on FortiGate.
696330	FortiManager may change all devices to *Managed FortiGate* when hiding all unauthorized devices, and it cannot be switched back.
696524	*Promote* button task does not work and hangs, if FortiManager cannot SSH access to HA cluster.
696730	FortiManager is unable to promote Secondary FortiGate as Primary in a HA Cluster.
698388	FortiManager cannot edit or create a static route with SD-WAN returning an error.

Bug ID	Description
705448	Device connection status may remain up after shutting down device port and updating device status.
713833	It may not be possible to rename device zone.
714611	Creating interface from VDOM may return *No Match Found* error.
718184	*AutoUpdate* with *unset options* and *unset post-lang* may cause device database and policy package status to display as *OUT-OF-SYNC*.
719968	*SD-WAN Monitor* should properly show the *Map View* of all devices.
724600	FortiManager may not be able to install static default route for SD-WAN from *Static route Template*.
725570	FortiManager may return *device can not be empty* error when creating or editing a static route on SD-WAN interface.
726167	Installing static route template may fail because interface is in another VDOM.
727123	*Meta Field* is not translating values with spaces into correct scripts.
728655	Configuration status may not be shown as *Synchronized* after installation.
728687	Policy package status may change to *Modified* on all FortiGate devices when a dynamic address group changes.
729301	A managed FortiGate with assigned CLI template remains in *Modified* state following a successful device configure installation.
729606	FortiManager should show where a Device Zone is used under Device Manager.
730482	CLI Template cannot add system DNS database entries if `set domain` contains the underscore character (_).
731204	FortiManager may incorrectly display *Object already exists* message while creating a new Hardware Switch interface.
731551	FortiManager may return error, *Failed to synchronize FortiAnalyzer with current ADOM data.Fail(errno=-3):Object does not exist*, when adding FortiAnalyzer devices.
732246	Clock format option no longer works to format date in TCL scripts.
733076	Model device links to real device may not work.
733080	Device status is shown as *Up* on GUI, even though there is no activity for the session between FortiManager and FortiGate.
733934	During zero-touch provisioning with *Enforce Firmware Version* enabled, upgrade task may hang if the connection is reset during the image transfer.
734487	Device's *hardware switch interface > physical interface member* may not save.
735106	Delete is spelled incorrectly when attempting to delete invalid host cluster device.
735402	When creating a new CLI Group Template and trying to add members to it, it does not allow users to select other *CLI Group Templates* that were already created.

Bug ID	Description
737025	*SD-WAN Monitor* widget may not be loaded when multiple performance SLAs are added.
737173	FortiManager should not unset *l2tp* and encapsulation with VPN phase2 interface.
739369	When revision history is very large, FortiManager may not be able to retrieve configuration.
739624	FortiManager should support FortiTester version 4.

FortiSwitch Manager

Bug ID	Description
684371	Clicking *OK* to import FortiSwitch Template results in no response.
714174	FortiSwitch manager DHCP reservation configuration may not synchronize correctly with FortiGate.
740936	FortiSwitch VLAN template creates unknown interface platform mapping.

Global ADOM

Bug ID	Description
667197	User should not be able to delete global object when ADOM is unlocked.
725763	Automatic install to ADOM devices may fail from Global ADOM.
728803	Copying global firewall policy may fail due to duplicate IPS sensors.
736541	NAT may stay as disabled on Global ADOM.
737381	FortiManager should not allow users to delete the default reserved address object starting with *g-*.
745772	FortiManager may randomly delete FortiManager IPv4 policies when assigning from the Global ADOM.

Others

Bug ID	Description
505795	FortiManager should allow users to configure the list of allowed TLS cipher suites.
510508	FortiManager cannot assign multiple ADOMs to an admin user via JSON API.

Bug ID	Description
697361	FortiExtender status may not be correctly displayed.
718251	Web Service with port 8080 disabled may still be in listening state.
731574	FortiManager may not be able to change web filter category action via JSON API.
732144	A CA certificate may be missing from some older FortiManager platforms causing failure to login with FortiCloud SSO.
733078	FortiManager may show multiple fmgd crashes with signal 11 segmentation fault.
733208	Users may not be able to login from GUI after restored database with changed HTTP or HTTPS port number.
736229	API may fail to promote unauthorized devices to a different ADOM.
738918	After upgrade, FortiManager may `set firewall-address 100000` on VDOM enabled FortiGate.
740523	Retrieve task may fail due to auto-update file already having been deleted by FGFM tunnel.
741118	Install policy package may hang at 50% with security console crash.
742137	FortiManager may return an error when running an Ansible script to configure network interfaces, zones, and policies.
744736	FGFM tunnel may go up and down with multiple `fgfmsd` crashes.
746311	`fgdsvr` process may crash when URL length is longer than 1024 characters.

Policy and Objects

Bug ID	Description
503978	*Thread Feeds* should be *Threat Feeds* on *Fabric Connector*.
549492	Load-balance type VIP cannot be displayed and saved correctly.
623346	In NGFW-policy policy package, FortiManager does not show *Security Virtual Wire Pair Policy* or *Virtual Wire Pair SSL Inspection & Authentication*.
644822	Imported SDN Connector objects may change to random names.
648970	If a profile group enables WAF or ICAP profile, the group should be hidden in flow-based policy.
657534	SSH and MAPI should not be supported in file filter profile protocol under flow mode.
666258	User should not be able to create a firewall policy with an Internet service with Destination direction in Source by using drag and drop.
690231	Where-used may fail to display references to certificate-inspection that were added to firewall policies in previous versions.

Bug ID	Description
690295	FortiManager may be slow when multiple users access GUI at the same time.
699975	Multiple filters are missing for Azure SDN Connector.
709908	When checking the status on AntiVirus profile, it may not show the correct inspection mode in list view when status stays in *flow-based (Full Scan)*.
710676	System replacement message group, `replacemsg-group auth-intf-quarantine`, does not exist.
710736	Classic Dual Pane mode cannot change left-panel size of object configuration.
714975	Imported groups or labels may not be available for direct use with policy.
716114	FortiManager should push changes in ssl-ssh-profile with *Untrusted SSL Certificates* setting reverted from *Block* to *Allow*.
719698	Performance for policy install may be slightly degraded after upgrading from 6.4.5 to 6.4.6.
720896	SSO admin with *Restricted Admin* profile should be able to view *Web Filter*, *Application Control*, or *IPS* objects.
722087	Edit user group with remote members on FortiManager GUI may cause unexpected change in `set group-name`.
724718	When FortiManager's NSX-T connector is executing an API request, it should not be limited to 50 records.
725024	*Proxy Policy* page shows empty when the *View Mode* is selected as *Interface Pair View*.
725132	When modifying IP address of Default VPN Interface of spoke in Device Manager, hub remote gateway should be modified to reflect that change.
725681	Under dual pane, scrolling may be available to move panels out of viewable area.
726077	Authentication Rules may run incorrect validation that prevents submission and results in an error: *The IP versions in source and destination addresses or Internet Services do not match*.
726548	`User-info-server` option is not available under dynamic mapping in CLI under user FSSO.
728689	FortiManager does not show warning or error while selecting *no-inspection* with UTM profile, which does not match FortiGate behavior.
728985	FortiManager may show signatures that have been deleted by FortiGuard.
729289	FortiManager should have an option to set `fortitoken/email/sms` to `unset` or `blank`.
729705	Installing policy requires Interface Validation for interfaces that are not being used in policy package.
730523	Unused policies tool may always generate a PDF containing all policies.
731053	FortiManager may miss some Internet Service entries.
732138	Non-full admin users should be able to export Policy Check and Unused Policy results.

Bug ID	Description
734556	FQDN type firewall address object can be created with an unsupported format.
735083	Policy packages' folders may not be displayed in alphabetical order.
735397	Cloned object's revision history information may not be related to the clone task.
735432	Users with ADOM-specified admin privilege may not be able to view policy package.
735738	When creating a VIP object with port forwarding filter, FortiManager may show an error.
735743	In classic dual pane, column settings are hidden by the object configuration pane.
738109	FortiManager may not install `auth-cert` from policy package to device.
738231	Creating VIP with IPv4 external IP mapped to IPv6 may trigger an error, *a.mappedip is undefined*.
738595	FortiManager may not correctly push AWS connector credentials.
738745	When an object is renamed, the new name must be used on all policies.
739205	FortiManager may thrown error *Cannot delete the only package or folder*, when deleting policy block.
740331	IP Pool details may be missing in ADOM v6.2.
740944	Custom IPS Signature script may fail to run on policy package or ADOM database.
742257	NPU log servers for hyperscale does not show up in policy package.
744591	Installing or importing IPS custom signature may fail when a signature's name contains a space character.
746273	Column filter may be extremely slow with large policy packages.
747330	FortiManager cannot assign or replace VIP with SD-WAN as source interface.
748523	After creating a VIP, FortiManager may not be able to choose the VIP on a policy.
748524	VIP is not visible in the policy, if the external interface is not the same as policy SD-WAN source interface.
749519	IPv4 policies in policy block may hidden on FortiManager's GUI.
750160	`custom-url-list` may not be correctly parsed when URLs contain space characters.

Revision History

Bug ID	Description
640714	FortiManager cannot correctly retrieve and import *interface subnet* type address showing *0.0.0.0* for IP.
642878	FortiManager should return a clear copy fail log for dynamic interface check error.

Bug ID	Description
643101	Copy may fail due to VIP overlapping when installing policy package.
674094	FortiManager may unset explicit proxy's HTTPS and PAC ports, and change the value to `0` instead.
674196	Installation may fail after editing or creating a firewall policy if `reputation-minimum` is set.
680549	Restricted user's *Quick Install* is not working correctly for Rating Overrides.
683728	Installation fails due to VIP mapped IP range error when installing v6.2 policy package to v6.4 device.
711314	VDOM specific *Disclaimer Page* configuration is purged from *default* replacemsg-group during Policy Package installation.
713552	If VIP address's source-filter list is too long, installation may fail.
722332	For AP Profile change, installation preview may show *No Entry*.
724340	FortiManager may unset `forward-error-correction` from FortiGate 7060E devices.
724647	After upgrading to 6.4, retrieval from a chassis may take a long time.
725252	When customer is trying to push policy package to a device group, installation window may not show any progress, but with a red cross.
725557	Install always try to delete hardware switch member interface causing installation failure.
725717	After upgrade, installation may fail due to `mcast-session-counting`.
728117	After upgrade, install may fail due to `set pri-type-max 1000000`.
728918	FortiManager should install changes applied on Global policy package and not indicate warnings like *no installing devices/no changes on package*.
729587	FortiManager may create an already deleted admin account on FortiGate when installing changes for a new VDOM.
733518	FortiManager may incorrectly move DNAT objects.
735455	FortiManager may try to delete thousands of policies during install.
735988	Switch and AP names may be reverted by controller status update from FortiGate.
740858	GCP project name must be set during install.
741543	Install may fail with unset MAC address on EMAC VLAN.
742242	Install fails after upgrade due to `set server-identity-check enable` on LDAP server configuration.
742806	When modifying a configuration and installing Device Settings only, FortiManager may not display the device's configuration change.
745715	FortiManager may not be able to install policy package with firewall rule using VIP group due to zone binding.
747837	FortiManager may try to delete interfaces lan1, lan2, and lan3, which are used by `virtual-switch.sw0` on FortiGate-40F.

Script

Bug ID	Description
630016	FortiGate user can see scripts from all ADOMs.
729571	TCL script commands run on device no longer show in the script log.
734942	Script includes static route with SD-WAN enabled may report error.
744030	FortiManager should not allow running script against device database with incorrect command.

Services

Bug ID	Description
685678	When FortiMail FIPS mode is enabled, FortiManager should be able to validate its license.
714127	Backup ADOM does not support firmware template upgrade.
725118	FortiManager may not log FortiGuard connectivity failures.
725721	FortiManager may not be able to recognize all FortiGate units within HA cluster, and it may not be able to provide update services to all units.
730877	The upgrade matrix file may be missing, and FortiManager is unable to calculate upgrade paths without the upgrade matrix file.
733174	FortiManager may not be able to recognize the object id 06002000NIDS02604 as IPS Signature Database(Extended).
733873	FortiManager may not get FortiGate HA cluster's contract information when Device Manager shows the secondary device's SN.
739625	FortiManager may not display licensing information for FortiTester.
741846	AP upgrade task may hang at 45%.

System Settings

Bug ID	Description
617601	*Sort by Time Used* in *Task Monitor* may not be correct.
663185	Search may not work for event logs in text mode.
690926	FortiManager removes SD-WAN field description upon ADOM upgrading from 6.2 to 6.4.

Bug ID	Description
696554	FortiManager may generate a lot of *cdb event log for object changed* event logs.
700608	The variable from meta data that is shown is not case sensitive, whereas the variable is case sensitive when using in a CLI template.
705145	*Username* is truncated to 49 characters in the notification Emails sent by FortiManager for workflow approvals.
711686	Workflow approval does not work when admin name has more than 49 characters.
722320	The *NOT search in advanced/text mode* search is not working for system event logs.
726007	Admin User systematically gets access to root ADOM in case of RADIUS authentication and *Fortinet-Vdom-Name* VSA is not set.
727233	ADOM license count should not count root ADOM.
728942	FortiManager may gray out some devices' tasks with error, which cannot be grouped together.
728991	Nested group search fails with *Bad search filter* if the user DN contains characters like "*,*" and "*()*".
729280	Admin User with no access to management ADOM or VDOM can create a new VDOM from non-management ADOM > VDOM.
735067	When creating a local account with the *Force this administrator to change password upon next log on* option checked, the setting should be applied for the first login.
736205	FortiManager may get stuck during upgrade.
738395	FortiManager tasks' time used should not be increased by timezone.
738622	ADOM upgrade from 6.0 to 6.2 may fail due to FortiExtender object.
743411	FortiManager should show more than five local certificates.

VPN Manager

Bug ID	Description
712633	VPN Manager pushes default `dpd-retrycount` and `dpd-retryinterval`, but it cannot display them.
712861	Policy Package Status stays *Synchronized* despite SSL-VPN Portal configuration being changed by using VPN Manager.
721783	Applying Authentication or Portal Mapping changes may take several minutes.
722924	FortiManager may not be able to edit `skip-check-for-unsupported-os enable` under SSL portal profile.

Known Issues

The following issues have been identified in 7.0.2. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
708100	AP Manager cannot show *Channels* when 160 MHz channel width is set.
749820	*AP Manager* > *SSID* > *Advanced Options* may not list objects under the settings `address-group`.

Device Manager

Bug ID	Description
545239	After adding FortiAnalyzer fabric ADOM to FortiManager, Device Manager's Log Status, Log Rate, or Device Storage column cannot get data from FortiAnalyzer.
554241	FortiManager cannot delete and reassign ports to VDOM when split VDOM is enabled.
610568	FortiManager may not follow the order in CLI Script template.
636638	Fabric view may get stuck at loading.
651560	SD-WAN monitor may get stuck loading when admin user belongs to device group.
660491	Device Manager system interface should not allow duplicated secondary IP address.
673548	May not be possible for FortiManager to change FortiGate interface settings when the interface type is "Software Switch".
674904	FortiManager may not be able to import policies with interface binding contradiction on `srcintf` error.
689721	When changing FortiGuard- related settings via CLI Configuration, FortiManager shows changes are reverted back, but it also shows the message: *Successfully updated*.
710570	`Any` statement is not accepted by FortiManager in the `prefix-list` configuration.
740893	Secondary IP may be purged when setting a description to VLAN interface.
729413	FortiManager is missing peer options with dial up user configuration with VPN IPSec Phase 1.

Bug ID	Description
748578	Retrieve FortiGate configuration may fail due to FSSO connector.
752443	Vertical scroll bar is missing in SD-WAN configuration.

FortiSwitch Manager

Bug ID	Description
674539	FortiManager may fail to upgrade two FortiSwitches at the same time.

Global ADOM

Bug ID	Description
691562	Threat feeds global objects are not installed to destination ADOM when using the *assign all* object option.

Others

Bug ID	Description
703585	FortiManager may return *Connection aborted* error with JSON API request.
729175	FortiManager should highlight device consisting of specific IP address under *Fabric View*.
732116	Setting of *FortiCloud Single Sign-On* is always displayed on login.
747716	JSON API does not return gateway for IPSec route.

Policy & Objects

Bug ID	Description
585177	FortiManager is unable to create VIPv6 virtual server objects.
615250	Search by CVE may not work for both IPS Signatures and IPS Filters.
646329	Policy Check may claim different IPS profiles as duplicate.
652753	Wen an obsolete internet service is selected, FortiManager may show entries' IDs instead of

Bug ID	Description
	names.
655601	FortiManager may be slow to add or remove a URL entry on web filter with a large list.
656991	FortiManager should not allow VIP to be created with same IP for External IP and Mapped IP Address.
659296	FortiManager may take a lot of time to update web filter URL filter list.
688586	Exporting Policy Package to *CSV* shows *certificate-inspection* in the *ssl-ssh-profile* column even when the profile is not in use.
713692	Web Filter Profile install may fail when using pre-defined URL filter.
719774	IP reputation for the policies are not working without source or destination.
720673	Many groups learned from Cisco ISE may be missing corresponding ADOM objects.
725427	Policy package install skips the policy where destination interface is set as SD-WAN zone and policy is IPSEC policy.
726105	*CLI Only Objects* may not be able to select FSSO interface.
729179	FortiManager may not be able to add Geography type address when interface mapping is enabled.
731037	There may be *File Filter* file type mismatch between FortiGate and FortiManager.
744766	FortiManager may not be able to retrieve IP address for group with NSX-T v3.1.2.
745863	FortiManager may display "*Invalid internet service source* error when selecting certain Internet services.
747558	FortiManager filters should work for *HitCounters*, *First Session*, and *Last session*.
748467	FortiManager does not have the same profiles as FortiGate with explicit proxy policy.
751710	Editing a global user FSSO object's dynamic mapping is not possible.

Revision History

Bug ID	Description
618305	FortiManager changes configuration system CSF settings.
635957	Install fails for subnet overlap IP between two interfaces.

Script

Bug ID	Description
384139	Filter does not work on device group.
654700	Users need to open *View Script Execution History* to see that TCL script fails.

Services

Bug ID	Description
753871	FortiClient packages should not continue to be received once the service for that firmware version has been disabled.

System Settings

Bug ID	Description
616703	GUI CLI Console may not respond.
640670	If a user-specified ADOM includes a global ADOM, workflow approval may not be able to find the same user.
652417	FortiManager HA may go out of synchronization periodically based on the logs.
721153	Scroll bar is missing from device drop-down list on ADOM overview page.
752916	FortiManager should be able to set desired permissions for Extender Manager in administrator profile settings.

VPN Manager

Bug ID	Description
615890	IPSec VPN `Authusergrp` option `Inherit from Policy` is missing when setting `xauthtype` as `auto server`.
699759	When installing a policy package, per-device mapped objects used in SSL VPN cannot be installed.

Appendix A - FortiGuard Distribution Servers (FDS)

In order for the FortiManager to request and retrieve updates from FDS, and for FortiManager to serve as a FDS, please configure the necessary settings on all devices between FortiManager and FDS, or between FortiManager and FortiGate devices based on the items listed below:

- FortiManager accesses FDS for antivirus and attack updates through TCP/SSL port 443.
- If there is a proxy server between FortiManager and FDS, FortiManager uses port 80 to communicate with the proxy server by default and connects to the proxy server using HTTP protocol.
- If FortiManager manages a FortiGate device located behind a proxy server, the proxy server permits TCP/SSL traffic to pass through via port 443.

FortiGuard Center update support

You can configure FortiManager as a local FDS to provide FortiGuard updates to other Fortinet devices and agents on your network. The following table lists which updates are available per platform/version:

Platform	Antivirus	WebFilter	Vulnerability Scan	Software
FortiClient (Windows)	✓	✓	✓	✓
FortiClient (Mac OS X)	✓		✓	
FortiMail	✓			
FortiSandbox	✓			
FortiWeb	✓			

Appendix B - Default and maximum number of ADOMs supported

This section identifies the supported number of ADOMs for FortiManager hardware models and virtual machines.

Hardware models

FortiManager supports a default number of ADOMs based on hardware model.

Some hardware models support an ADOM subscription license. When you purchase an ADOM subscription license, you increase the number of supported ADOMs. For example, you can purchase an ADOM subscription license for the FMG-3000G series, which allows you to use up to a maximum of 8000 ADOMs.

Other hardware models do not support the ADOM subscription license. For hardware models that do not support the ADOM subscription license, the default and maximum number of ADOMs is the same.

FortiManager Platform	Default number of ADOMs	ADOM license support?	Maximum number of ADOMs
200G Series	30		30
300F Series	100		100
400G Series	150		150
1000F Series	1000		1000
2000E Series	1200		1200
3000G Series	4000	✓	8000
3700G Series	10,000	✓	10,000

For FortiManager F series and earlier, the maximum number of ADOMs is equal to the maximum devices/VDOMs as described in the FortiManager Data Sheet.

Virtual Machines

FortiManager VM subscription license includes five (5) ADOMs. Licenses are non-stackable. Additional ADOMs can be purchased with an ADOM subscription license.

For FortiManager VM perpetual license, the maximum number of ADOMs is equal to the maximum number of Devices/VDOMs listed in the FortiManager Data Sheet.

www.fortinet.com